

DGPeterson, LLC

HIPAA Privacy & Security Consulting

HIPAA Security Auditors Report

Prepared for: Vigilant Medical, LLC
Date: January 28, 2011

DGPeterson, LLC

HIPAA Privacy & Security Consulting

January 28, 2011

Santosh Venkatesha, CEO
Vigilant Medical, LLC
3600 Clipper Mill Road
Suite 410
Baltimore, MD 21211

ImageShare HIPAA Security Auditors Report

We have examined the accompanying areas of audit emphasis as it relates to Vigilant Medical's software program (ImageShare) controls of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) technical safeguards of the security standards. Our examination included procedures to obtain reasonable assurance that -

1. The accompanying areas of audit emphasis (HIPAA technical safeguards of the security standards) presents fairly, in all material respects, the aspects of Vigilant Medical's policies, procedures and controls that may be relevant to a user organization's security of the ImageShare program as it relates to HIPAA.
2. That HIPAA policies and procedures included in the areas of audit emphasis were suitably designed to achieve the control objectives specified in the compliance program, if those policies and procedures were complied with satisfactorily.

Our examination was performed applying HIPAA Administration Simplification, Part 164 Security Standards, National Institute of Standards and Technology, Special Publication 800-66, Revision 1 and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion. Attached is the U.S. Department of Health and Human Services, Office for Civil Rights, HIPAA Administrative Simplification, Regulation Text, 45 CFR 160,162 and 164 Unofficial Version as amended through February 16, 2006 and National Institute of Standards and Technology, Special Publication 800-66, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.

The accompanying areas of audit emphasis include only the relevant HIPAA security standards as it relates to Vigilant Medical's ImageShare software program and does not extend to users of Vigilant Medical's ImageShare program. The security standards objectives were specified by Vigilant Medical.

In our opinion, the accompanying areas of audit emphasis relating to Vigilant Medical's HIPAA policies and procedures presents fairly, in all material respects, the relevant aspects of Vigilant Medical's HIPAA compliance program that had been in operation on January 28th 2011. Also, in our opinion, the policies and procedures, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described standards were complied with satisfactorily.

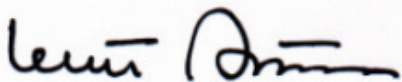
The relative effectiveness and significance of specific HIPAA policies and procedures of Vigilant Medical's ImageShare software program and their effect on assessments of control risk at user organizations are dependent on their interaction with internal control, and other factors present at individual user organizations. We have performed no procedures to evaluate the effectiveness of internal controls at individual user organizations.

The results of analyzing HIPAA policies and procedures of Vigilant Medical's ImageShare program were determined as of January 28, 2011. Any projection of such information to the future is subject to the risk that, because of change, the areas of audit emphasis or controls may no longer portray the compliance program in existence. The potential effectiveness of specific policies and procedures at Vigilant Medical are subject to inherent limitations resulting from non-compliance. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the compliance program or policies and procedures, (2) changes in implementation of policies and procedures, or (3) changes required because of the passage of time may alter the validity of such conclusions.

This report is intended solely for use by management of Vigilant Medical.

We appreciate this opportunity to discuss the contents of this report and answer any questions you may have about these or any other audit-related matters.

Sincerely,

A handwritten signature in black ink, appearing to read "Grant Peterson".

Grant Peterson, J.D.
Principal

EXECUTIVE SUMMARY

Vigilant Medical's has developed a new web-based file sharing service allowing doctors to upload and download images without installing any special software. Imaging studies play a large role in determining patient care in many fields of medicine. Often, doctors in cardiology will share echocardiograms, MRI's, and CAT scans with each other and specialists in the field to determine the right diagnosis and course of care. Currently, several software programs allow doctors to electronically share imaging studies. However, these files are often compressed and many programs do not accept the full range of imaging studies. This limits the ability of specialists to quickly and accurately make a diagnosis. The low-resolution image transmitted through many web-based systems delays receiving and prevents prompt therapeutic recommendations for the patient. In addition, there may be added expense to the patient and healthcare system, as patients remain in the hospital awaiting decisions for their medical care.

Vigilant Medical's ImageShare software program allows healthcare organizations to simply insert a CD or DVD into their computer, then directed to Vigilant's secure website. The software automatically recognizes the imaging study and transfers these images to Vigilant's cloud computing platform which ensures the confidentiality, integrity, and availability of data, while providing consultants with the ability to review an image file and even share them with their colleagues. Unlike other programs, ImageShare does not compress the file size, allowing consulting physicians to view exactly the same data, and even download the study to their own workstation and PACS. It also allows a full range of imaging studies to be shared and it maintains the DICOM file structure – a standard in the medical industry for medical imagery. In addition, doctors are free to use any medical imaging viewer they prefer to review the study.

In November 2010, Vigilant Medical management engaged DGPeterson, LLC, a HIPAA privacy and security consulting firm to examine the compliance controls in place as it relates to Vigilant Medical's ImageShare software program and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) security standards. Our examination included procedures to obtain reasonable assurance about whether

1. The accompanying areas of audit emphasis (HIPAA privacy and security standards) presents fairly, in all material respects, the aspects of Vigilant Medical's ImageShare policies, procedures and controls that may be relevant to a user organization's security as it relates to HIPAA.
2. That HIPAA policies and procedures included in the areas of audit emphasis were suitably designed to achieve the control objectives specified in the compliance program, if those policies and procedures were complied with satisfactorily.

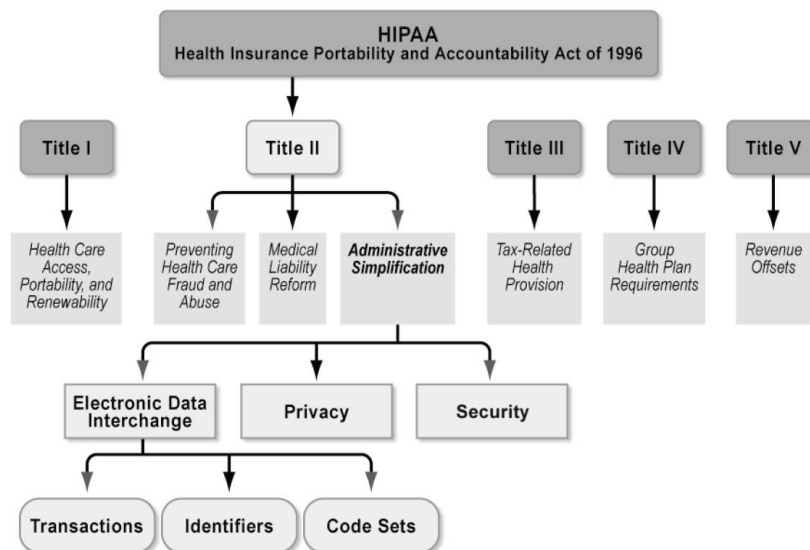
Our examination was performed applying HIPAA Administration Simplification, Part 164 Security and Privacy Standards, National Institute of Standards and Technology, Special Publication 800-66, Revision 1 and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion. Attached is the U.S. Department of Health and Human Services, Office for Civil Rights, HIPAA Administrative Simplification, Regulation Text, 45 CFR 160,162 and 164 Unofficial Version as amended through February 16, 2006 and National Institute of Standards and Technology, Special Publication 800-66, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.

The accompanying areas of audit emphasis include only the relevant HIPAA security standards as it relates to Vigilant Medical's ImageShare software program and does not extend to customers of Vigilant Medical. The security standards objectives were specified by Vigilant Medical.

About the Health Insurance Portability and Accountability Act (HIPAA)

In 1996, Congress enacted the Health Insurance Portability and Accountability Act (HIPAA), of which the Administrative Simplification provisions promote efficiency in

the healthcare industry through the use of transaction standards for the exchange of health information, privacy standards, and security standards for the use and disclosure of individually identifiable health information. This audit relates only to the technical safeguard security components of HIPAA.



HIPAA Security Components

HIPAA Security regulations are composed of multiple parts, each containing its own specific rules and standards and include:

Security - Standards for Security of Health Information - The Security rule for health information includes administrative, technical, and physical safeguards to ensure the integrity, confidentiality, and availability of health information and to protect against security violations and unauthorized use or disclosure of health information. The Security rule relates specifically to electronic PHI (or ePHI) and protection of ePHI data from unauthorized access.

Security standards became effective April 20, 2005.

General Rules and Scope of Security Standard

The Security rule adopts national standards for safeguards to protect the confidentiality, integrity, and availability of electronic protected health information of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Confidentiality is designed to assure that data or information is not made available or disclosed to unauthorized persons or processes. Integrity is the function designed to assure that data or information has not been altered or destroyed in an unauthorized manner. Availability is the function that assures that data or information is accessible and usable upon demand by an authorized person. However, under HIPAA, the determination of the specific mechanisms and the specific security features to be implemented remains a business decision in many cases.

Comprehensive, Scalable, Technology Neutral

The security standard is based on three basic HIPAA concepts. First, the standard is comprehensive and coordinated to address all aspects of security. Second, it is scalable, so that it can be effectively implemented by covered entities of all types and sizes. Third, it is not linked to specific technologies, allowing covered entities to make use of future technology advancements.

Administrative, Physical and Technical safeguards

The security standards define the administrative, physical, and technical safeguards required to protect electronic protected health information. The standards also require covered entities to implement safeguards to protect electronic protected health information from unauthorized access, alteration, deletion, and transmission.

The Privacy Rule, by contrast, sets standards for how protected health information should be controlled by setting forth what uses and disclosures are authorized or required and what rights patients have with respect to their health information.

The security standard sets a baseline, or minimum level, of security measures that must be taken by a covered entity and stipulates that a business associate must also

implement reasonable and appropriate safeguards, through a Business Associate Agreement.

Required or Addressable

Within the Security Rule sections, many of the standards contain implementation specifications. An implementation specification is a more detailed description of the method or approach covered entities can use to meet a particular standard. Implementation specifications are either “required” or “addressable”. A required implementation specification is similar to a standard, in that a covered entity must comply with it. Specifications that are addressable require covered entities to perform an assessment in order to determine whether the implementation specification is a reasonable and appropriate safeguard for implementation in the covered entity’s environment.

Audit Emphasis: HIPAA Security

Technical Safeguards

Vigilant Medical’s ImageShare software program serves as one element in the wider group of systems, business units and users in the delivery of healthcare imaging service. As a result, each element of the healthcare delivery system has a shared responsibility in performing required HIPAA compliance they control. To that end, Vigilant Medical has applied the “technical safeguards” of the security rule to the ImageShare program, over which they have control and must rely on the wider group of systems, business units and users to assume the responsibility and management of HIPAA compliance in those areas they control.

Vigilant Medical has created internal security compliance controls for their ImageShare software program designed to provide reasonable assurance that their organization has complied with HIPAA technical safeguard standards. Our examination included procedures to obtain reasonable assurance that -

The accompanying areas of audit emphasis (HIPAA technical safeguards security standards) presents fairly, in all material respects, the aspects of Vigilant Medical’s ImageShare software program policies, procedures and controls that may be relevant to a user organization’s security as it relates to HIPAA.

That HIPAA policies and procedures included in the areas of audit emphasis were suitably designed to achieve the control objectives specified in the compliance program, if those policies and procedures were complied with satisfactorily.

Our examination was performed applying National Institute of Standards and Technology, Special Publication 800-66, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (technical safeguards) in analyzing Vigilant Medical's ImageShare policies, procedures and controls we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

Audit Emphasis Standard and Section	Implementation Specifications (R)=Required, (A)= Addressable	Control Objectives
<div> <div>HIPAA Security</div> <div>Technical Safeguards</div> </div>		
Access Control 164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)	Suitably Designed
Audit Controls 164.312(b)	(R)	Suitably Designed
Integrity 164.312 (c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)	Suitably Designed
Person or Entity Authentication 164.312(d)	(R)	Suitably Designed
Transmission Security 164.312(e)(1)	Integrity Controls (A) Encryption (A)	Suitably Designed